

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Tatuya JINMEI, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: COMMUNICATION SCHEME FOR PREVENTING ATTACK BY PRETENDING IN SERVICE
USING ANYCAST

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**:
Application No. Date Filed

- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-329950	November 13, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年11月13日
Date of Application:

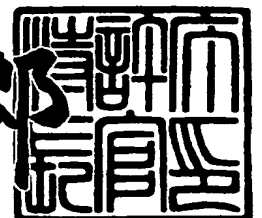
出願番号 特願2002-329950
Application Number:
[ST. 10/C]: [JP 2002-329950]

出願人 株式会社東芝
Applicant(s):

2003年 7月 8日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3053996

【書類名】 特許願

【整理番号】 13B027068

【提出日】 平成14年11月13日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/56

【発明の名称】 通信装置、境界ルータ装置、サーバ装置、通信システム
、通信方法、ルーティング方法、通信プログラム及びルー
ーティングプログラム

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
 研究開発センター内

 【氏名】 神明 達哉

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
 研究開発センター内

 【氏名】 石山 政浩

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
 研究開発センター内

 【氏名】 玉田 雄三

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100083806

 【弁理士】

 【氏名又は名称】 三好 秀和

 【電話番号】 03-3504-3075

【選任した代理人】

【識別番号】 100068342

【弁理士】

【氏名又は名称】 三好 保男

【選任した代理人】

【識別番号】 100100712

【弁理士】

【氏名又は名称】 岩▲崎▼ 幸邦

【選任した代理人】

【識別番号】 100100929

【弁理士】

【氏名又は名称】 川又 澄雄

【選任した代理人】

【識別番号】 100108707

【弁理士】

【氏名又は名称】 中村 友之

【選任した代理人】

【識別番号】 100095500

【弁理士】

【氏名又は名称】 伊藤 正和

【選任した代理人】

【識別番号】 100101247

【弁理士】

【氏名又は名称】 高橋 俊一

【選任した代理人】

【識別番号】 100098327

【弁理士】

【氏名又は名称】 高松 俊雄

【手数料の表示】**【予納台帳番号】** 001982**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 通信装置、境界ルータ装置、サーバ装置、通信システム、通信方法、ルーティング方法、通信プログラム及びルーティングプログラム

【特許請求の範囲】

【請求項 1】 所定の宛先アドレス宛にパケットを送信する送信手段と、
前記パケットの応答として応答パケットを受信する受信手段と、
受信した前記応答パケットに含まれる送信元アドレスを検出する第 1 の検出手段と、

検出した前記送信元アドレスが前記宛先アドレスと異なる場合、前記応答パケットに含まれる、前記宛先アドレスを持つ他の通信装置がエニキャストアドレスを付与されていることを示す識別子を検出する第 2 の検出手段と、

検出した前記識別子に基づいて前記応答パケットの検証を行う検証手段とを具備したことを特徴とする通信装置。

【請求項 2】 エニキャストアドレスを持つサーバ装置が属する第 1 のネットワークと第 2 のネットワークとの境界に位置する境界ルータ装置であって、

前記第 2 のネットワーク側の通信装置から所定のエニキャストアドレスを持つ前記サーバ装置宛のパケットを受信する第 1 の受信手段と、

前記パケットを前記サーバ装置に転送する第 1 の転送手段と、

前記サーバ装置から前記パケットに対する応答パケットを受信する第 2 の受信手段と、

前記応答パケットに含まれる、前記エニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出する検出手段と、

前記検出手段において前記識別子が検出された場合、予め保持している前記第 2 のネットワーク内における前記エニキャストアドレスを持つサーバ装置に関する情報に基づいて、前記応答パケットが前記サーバ装置から送信された応答パケットであることを検証する検証手段と、

この検証手段の結果に基づいて、前記応答パケットを前記通信装置に転送するか否かを制御する転送制御手段と、

前記制御手段にて前記パケットを転送すると判断した場合には前記応答パケッ

トを前記通信装置に転送する第2の転送手段

とを具備したことを特徴とする境界ルータ装置。

【請求項3】 第1のネットワークに接続され、所定のエニキャストアドレスを持つサーバ装置において、

第2のネットワーク側に接続された通信装置から前記エニキャストアドレス宛に送信されたパケットを受信する受信手段と、

前記パケットに応答する応答パケットに、この応答パケットの送信元がエニキャストアドレスを持つことを示す識別子を付与する識別子付与手段と

前記応答パケットを前記通信装置へ送信する送信手段

とを具備したことを特徴とするサーバ装置。

【請求項4】 所定のエニキャストアドレスを持ち第1のネットワークに接続されたサーバ装置と、第2のネットワークに接続された通信装置と、前記第1のネットワークと前記第2のネットワークとの境界に位置する境界ルータ装置とからなる通信システムにおいて、前記通信装置は、

前記エニキャストアドレス宛にパケットを送信する第1の送信手段、

前記パケットの応答として前記サーバから応答パケットを受信する第1の受信手段とを具備し、前記サーバ装置は、

前記通信装置から前記エニキャストアドレス宛に送信された前記パケットを受信する第2の受信手段、

前記パケットに応答する前記応答パケットに、前記サーバ装置がエニキャストアドレスを持つことを示す識別子を付与する識別子付与手段、

前記応答パケットを前記通信装置へ送信する第2の送信手段

とを具備し、前記境界ルータ装置は、

前記通信装置から所定のエニキャストアドレスを持つ前記サーバ装置宛のパケットを受信する第3の受信手段、

前記パケットを前記サーバ装置に転送する第1の転送手段、

前記サーバ装置から前記パケットに対する応答パケットを受信する第4の受信手段、

前記応答パケットに含まれる、前記エニキャストアドレスとは異なる送信元ア

ドレスが付与されていることを示す識別子を検出する検出手段、

前記検出手段において前記識別子が検出された場合、予め保持している前記第1のネットワーク内における前記エニキャストアドレスを持つサーバ装置に関する情報に基づいて、前記応答パケットが前記サーバから送信された応答パケットであることを検証する検証手段、

前記検証手段の結果に基づいて、前記応答パケットを前記通信装置に転送するか否かを制御する転送制御手段、

前記制御手段にて前記パケットを転送すると判断した場合には前記応答パケットを前記通信装置に転送する第2の転送手段

とを具備したことを特徴とする通信システム。

【請求項5】 所定の宛先アドレス宛にパケットを送信し、
前記パケットの応答として応答パケットを受信し、
受信した該応答パケットに含まれる該応答パケットの送信元アドレスを検出し、

検出した前記送信元アドレスが、前記宛先アドレスと異なる場合、前記応答パケットに含まれる、この応答パケットを送信した他の通信装置がエニキャストアドレスを持つことを示す識別子を検出し、

前記識別子に基づいて前記応答パケットの検証を行う
ことを特徴とする通信方法。

【請求項6】 エニキャストアドレスを持つサーバ装置が属する第1のネットワークと第2のネットワークとの境界に位置する境界ルータ装置におけるルーティング方法であって、

前記第2のネットワーク側の通信装置から所定のエニキャストアドレスを持つ前記サーバ装置宛のパケットを受信し、

前記パケットを前記サーバ装置に転送し、

前記サーバ装置から前記パケットに対する応答パケットを受信し、

前記応答パケットに含まれる、前記エニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出し、

前記識別子が検出された場合、予め保持している前記第2のネットワーク内に

おける前記エニキャストアドレスを持つサーバ装置に関する情報に基づいて、前記応答パケットが前記サーバ装置から送信された応答パケットであることを検証し、

この検証の結果に基づいて、前記応答パケットを前記通信装置に転送するか否かを制御する

ことを特徴とするルーティング方法。

【請求項 7】 第 1 のネットワークに接続され、所定のエニキャストアドレスを持つサーバ装置における通信方法であって、

第 2 のネットワーク側に接続された通信装置から前記エニキャストアドレス宛に送信されたパケットを受信し、

前記パケットに応答する応答パケットに、前記サーバ装置がエニキャストアドレスを持つことを示す識別子を付与し、

前記応答パケットを前記通信装置へ送信する

ことを特徴とする通信方法。

【請求項 8】 所定の宛先アドレス宛にパケットを送信し、

前記パケットの応答として応答パケットを受信し、

受信した該応答パケットに含まれる該応答パケットの送信元アドレスを検出し、

検出した前記送信元アドレスが、前記宛先アドレスと異なる場合、前記応答パケットに含まれる、この応答パケットを送信した他の通信装置がエニキャストアドレスを持つことを示す識別子を検出し、

前記識別子に基づいて前記応答パケットの検証を行う

ことをコンピュータに実行させる為の通信プログラム。

【請求項 9】 エニキャストアドレスを持つサーバ装置が属する第 1 のネットワークと第 2 のネットワークとの境界に位置する境界ルータ装置においてルーティング処理を行うコンピュータに、

前記第 2 のネットワーク側の通信装置から所定のエニキャストアドレスを持つ前記サーバ装置宛のパケットを受信し、

前記パケットを前記サーバ装置に転送し、

前記サーバ装置から前記パケットに対する応答パケットを受信し、
前記応答パケットに含まれる、前記エニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出し、
前記識別子が検出された場合、予め保持している前記第2のネットワーク内における前記エニキャストアドレスを持つサーバ装置に関する情報に基づいて、前記応答パケットが前記サーバ装置から送信された応答パケットであることを検証し、
この検証の結果に基づいて、前記応答パケットを前記通信装置に転送するか否かを制御する

ことを実行させる為のルーティングプログラム。

【請求項10】 第1のネットワークに接続され、所定のエニキャストアドレスを持つサーバ装置において通信を行うコンピュータに、

第2のネットワーク側に接続された通信装置から前記エニキャストアドレス宛に送信されたパケットを受信し、

前記パケットに応答する応答パケットに、前記サーバ装置がエニキャストアドレスを持つことを示す識別子を付与し、

前記応答パケットを前記通信装置へ送信する
ことを実行させる為の通信プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、IPv6のエニキャストアドレスを用いた環境における応答のなりすましを防止する技術に係り、通信装置、境界ルータ装置、サーバ装置、通信システム、通信方法、ルーティング方法、通信プログラム及びルーティングプログラムに関する。

【0002】

【従来の技術】

近年、世界最大のコンピュータネットワーク「インターネット (Internet)」の利用が普及してきており、インターネットと接続し、公開された情報やサービ

スを利用したり、逆にインターネットを通じてアクセスしてくる外部ユーザに対し、情報やサービスを提供することで、新たなコンピュータビジネスが開拓されている。

【0003】

またインターネットにおいて利用される新たな技術の開発が活発に行われている。インターネットでは、接続された各計算機（ノード、サーバなど）がそれぞれIPアドレスという識別子を持ち、このIPアドレスを元にパケットの交換により通信が行われる。

【0004】

IPアドレスの形式はIPv4と呼ばれる32ビット長のアドレス体系が用いられていたが、近年新たにIPv6と呼ばれる128ビット長のアドレス体系に移行しつつある。

【0005】

このIPv6の特徴の一つに、エニキャストアドレスの導入が挙げられる。エニキャストアドレスは、経路制御上はユニキャストと同様に利用されるが、ユニキャストアドレスと異なり、複数ノード上の複数インターフェースに割り当てられる。

【0006】

したがって、あるノードからエニキャストアドレス宛に出したパケットは、経路上最も近いノードに配送される。仮にエニキャストアドレスを割り当てられたノードに不良が生じたとしても、経路情報が収束した後に、同じアドレスを持つ次善のルータへ自動的に切り替えることができる。

【0007】

エニキャストアドレスの持つこうした特性を利用して、あるサービスを提供する複数のサーバに既知のエニキャストアドレスを割り当てることにより、エンドホストに特別な設定や変更を施さずに冗長性の高いサービスが実現できる。

【0008】

ただし、IPv6のエニキャストアドレスは、送信元アドレスとして使ってはいけないという制限が課せられている。したがって、エニキャストアドレス宛の

パケットを受け取ったサーバは、応答を返すときには自身のユニキャストアドレスを送信元アドレスとして用いる必要がある。

【0009】

ここで、一般的にユニキャストアドレスを利用する場合には、「なりすまし」による悪意の第三者からの攻撃を受けやすくなる。ユニキャストアドレス宛にパケットを出すクライアント端末にとって、応答を返すサーバのユニキャストアドレスを事前に知ることはできないので、どのような送信元アドレスを持つ応答パケットであっても受け入れなければならない。

【0010】

このため、実際にはサービスを提供する権限を持たないノードからの不正な「なりすまし」による応答であっても、クライアント端末が受け入れてしまう可能性という問題があった。

【0011】

またユニキャストアドレスを用いたサービスでは、たとえば、問い合わせパケットの宛先と応答パケットの送信元を比較する、といった簡単な検証方法があり、実際に利用されてもいる。

【0012】

送信元アドレスを偽ること自体は容易であるため、これは完全な検証とはなり得ない。しかし、たとえば、ネットワーク境界のルータで送信元アドレスに対する正当性検証を行うフィルタリングと併用することで、攻撃を受ける範囲をある程度狭めることはできる。

【0013】

しかしながらユニキャストアドレスの場合には、送信元アドレスを偽ることなく不正な応答を返すことができるため、なりすましによる悪意の第三者からの攻撃を受ける可能性がユニキャストを用いた場合よりも高くなってしまうという問題があった。

【0014】

【非特許文献1】

IETF RFC2460 Internet Protocol, Version 6 (IPv6) Specification

, December 1998

【0015】

【発明が解決しようとする課題】

前述したように、IPv6におけるユニキャストアドレスを用いたサービスでは、そのユニキャストアドレスを持った送信元の送信元アドレスに、ユニキャストアドレスを使うことができないという制約があるために、送信元の正当性を検証することが困難であるという問題があった。

【0016】

この場合、悪意の第三者による送信元アドレスの改ざんにより、なりすましによる攻撃を受ける可能性がユニキャストを用いた場合よりも高くなってしまう危険性があった。

【0017】

本発明は、上記問題点を解決する為になされたものであり、ユニキャストアドレスを用いたサービスにおいて、送信元の正当性を検証することにより、なりすましによる被害を防止する為の通信装置、境界ルータ装置、サーバ装置、通信システム、通信方法、ルーティング方法、通信プログラム及びルーティングプログラムに関する。

【0018】

【課題を解決するための手段】

本発明の第1の特徴は、(イ) 所定の宛先アドレス宛にパケットを送信する送信手段と、(ロ) パケットの応答として応答パケットを受信する受信手段と、(ハ) 受信した応答パケットに含まれる送信元アドレスを検出する第1の検出手段と、(ニ) 検出した送信元アドレスが宛先アドレスと異なる場合、応答パケットに含まれる、宛先アドレスを持つ他の通信装置がユニキャストアドレスを付与されていることを示す識別子を検出する第2の検出手段と、(ホ) 検出した識別子に基づいて応答パケットの検証を行う検証手段とを具備する通信装置であることを要旨とする。

【0019】

上記の発明によると、通信装置は、応答パケット及びその送信元アドレスによ

り、応答パケットが適切なサーバ等より送信されているか否かを明らかにすることができる。

【0020】

本発明の第2の特徴は、(イ) エニキャストアドレスを持つサーバ装置が属する第1のネットワークと第2のネットワークとの境界に位置する境界ルータ装置であって、第2のネットワーク側の通信装置から所定のエニキャストアドレスを持つサーバ装置宛のパケットを受信する第1の受信手段と、(ロ) パケットをサーバ装置に転送する第1の転送手段と、(ハ) サーバ装置からパケットに対する応答パケットを受信する第2の受信手段と、(ニ) 応答パケットに含まれる、エニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出する検出手段と、(ホ) 検出手段において識別子が検出された場合、予め保持している第2のネットワーク内におけるエニキャストアドレスを持つサーバ装置に関する情報に基づいて、応答パケットがサーバ装置から送信された応答パケットであることを検証する検証手段と、(ヘ) この検証手段の結果に基づいて、応答パケットを通信装置に転送するか否かを制御する転送制御手段と、(ト) 制御手段にてパケットを転送すると判断した場合には応答パケットを通信装置に転送する第2の転送手段とを具備する境界ルータ装置であることを要旨とする。

【0021】

上記の発明によると、境界ルータ装置は、応答パケット及びその送信元アドレスにより、応答パケットが適切なサーバ等より送信されているか否かを明らかにすることができる。

【0022】

本発明の第3の特徴は、(イ) 第1のネットワークに接続され、所定のエニキャストアドレスを持つサーバ装置において、第2のネットワーク側に接続された通信装置からエニキャストアドレス宛に送信されたパケットを受信する受信手段と、(ロ) パケットに応答する応答パケットに、この応答パケットの送信元がエニキャストアドレスを持つことを示す識別子を付与する識別子付与手段と、(ハ) 応答パケットを通信装置へ送信する送信手段とを具備するサーバ装置であるこ

とを要旨とする。

【0023】

上記の発明によると、サーバ装置がエニキャスト通信を示す識別子を付与することが可能となる。ひいては、応答パケットを送受信する他の装置が適切なサーバ等より送信された応答パケットか否かを判断することができる。

【0024】

本発明の第4の特徴は、(イ) 所定のエニキャストアドレスを持ち第1のネットワークに接続されたサーバ装置と、第2のネットワークに接続された通信装置と、第1のネットワークと第2のネットワークとの境界に位置する境界ルータ装置とからなる通信システムにおいて、(ロ) 通信装置は、エニキャストアドレス宛にパケットを送信する第1の送信手段、(ハ) パケットの応答としてサーバから応答パケットを受信する第1の受信手段とを具備し、(ニ) サーバ装置は、通信装置からエニキャストアドレス宛に送信されたパケットを受信する第2の受信手段、(ホ) パケットに応答する応答パケットに、サーバ装置がエニキャストアドレスを持つことを示す識別子を付与する識別子付与手段、(ヘ) 応答パケットを通信装置へ送信する第2の送信手段とを具備し、(ト) 境界ルータ装置は、通信装置から所定のエニキャストアドレスを持つサーバ装置宛のパケットを受信する第3の受信手段、(チ) パケットをサーバ装置に転送する第1の転送手段、(リ) サーバ装置からパケットに対する応答パケットを受信する第4の受信手段、(ヌ) 応答パケットに含まれる、エニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出する検出手段、(ル) 検出手段において識別子が検出された場合、予め保持している第1のネットワーク内におけるエニキャストアドレスを持つサーバ装置に関する情報に基づいて、応答パケットがサーバから送信された応答パケットであることを検証する検証手段、(ヲ) 検証手段の結果に基づいて、応答パケットを通信装置に転送するか否かを制御する転送制御手段、(ワ) 制御手段にてパケットを転送すると判断した場合には応答パケットを通信装置に転送する第2の転送手段とを具備する通信システムであることを要旨とする。

【0025】

上記の発明によると、サーバ装置が付与したユニキャスト通信を示す識別子を、通信装置及び境界ルータ装置が検知、判断することより、ユニキャストアドレスを用いた通信システムと同様の安全性をユニキャストアドレスを用いた通信システムにて確保することができる。

【0026】

本発明の第5の特徴は、(イ) 所定の宛先アドレス宛にパケットを送信し、(ロ) パケットの応答として応答パケットを受信し、(ハ) 受信した応答パケットに含まれる応答パケットの送信元アドレスを検出し、(ニ) 検出した送信元アドレスが、宛先アドレスと異なる場合、応答パケットに含まれる、この応答パケットを送信した他の通信装置がユニキャストアドレスを持つことを示す識別子を検出し、(ホ) 識別子に基づいて応答パケットの検証を行う通信方法であることを要旨とする。

【0027】

本発明の第6の特徴は、(イ) ユニキャストアドレスを持つサーバ装置が属する第1のネットワークと第2のネットワークとの境界に位置する境界ルータ装置におけるルーティング方法であって、第2のネットワーク側の通信装置から所定のユニキャストアドレスを持つサーバ装置宛のパケットを受信し、(ロ) パケットをサーバ装置に転送し、(ハ) サーバ装置からパケットに対する応答パケットを受信し、(ニ) 応答パケットに含まれる、ユニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出し、(ホ) 識別子が検出された場合、予め保持している第2のネットワーク内におけるユニキャストアドレスを持つサーバ装置に関する情報に基づいて、応答パケットがサーバ装置から送信された応答パケットであることを検証し、(ヘ) この検証の結果に基づいて、応答パケットを通信装置に転送するか否かを制御するルーティング方法であることを要旨とする。

【0028】

本発明の第7の特徴は、(イ) 第1のネットワークに接続され、所定のユニキャストアドレスを持つサーバ装置における通信方法であって、(ロ) 第2のネットワーク側に接続された通信装置からユニキャストアドレス宛に送信されたパケ

ットを受信し、(ハ) パケットに応答する応答パケットに、サーバ装置がエニキャストアドレスを持つことを示す識別子を付与し、(ニ) 応答パケットを通信装置へ送信する通信方法であることを要旨とする。

【0029】

本発明の第8の特徴は、(イ) 所定の宛先アドレス宛にパケットを送信し、(ロ) パケットの応答として応答パケットを受信し、(ニ) 受信した応答パケットに含まれる応答パケットの送信元アドレスを検出し、(ホ) 検出した送信元アドレスが、宛先アドレスと異なる場合、応答パケットに含まれる、この応答パケットを送信した他の通信装置がエニキャストアドレスを持つことを示す識別子を検出し、(ヘ) 識別子に基づいて応答パケットの検証を行うことをコンピュータに実行させる為の通信プログラムであることを要旨とする。

【0030】

本発明の第9の特徴は、(イ) エニキャストアドレスを持つサーバ装置が属する第1のネットワークと第2のネットワークとの境界に位置する境界ルータ装置においてルーティング処理を行うコンピュータに、第2のネットワーク側の通信装置から所定のエニキャストアドレスを持つサーバ装置宛のパケットを受信し、(ロ) パケットをサーバ装置に転送し、(ハ) サーバ装置からパケットに対する応答パケットを受信し、(ニ) 応答パケットに含まれる、エニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出し、(ホ) 識別子が検出された場合、予め保持している第2のネットワーク内におけるエニキャストアドレスを持つサーバ装置に関する情報に基づいて、応答パケットがサーバ装置から送信された応答パケットであることを検証し、(ヘ) この検証の結果に基づいて、応答パケットを通信装置に転送するか否かを制御することを実行させる為のルーティングプログラムであることを要旨とする。

【0031】

本発明の第10の特徴は、(イ) 第1のネットワークに接続され、所定のエニキャストアドレスを持つサーバ装置において通信を行うコンピュータに、第2のネットワーク側に接続された通信装置からエニキャストアドレス宛に送信されたパケットを受信し、(ロ) パケットに応答する応答パケットに、サーバ装置がエ

ニキャストアドレスを持つことを示す識別子を付与し、(ハ) 応答パケットを通信装置へ送信することを実行させる為の通信プログラムであることを要旨とする。

【0032】

【発明の実施の形態】

(通信システム)

始めに、エニキャストアドレスを用いたネットワーク及び通信システムの概要について説明する。通信システム100は、図1に示すように、第2のネットワーク9内に位置する通信装置10a、10b、10c、…、インターネット1、境界ルータ20、Aルータ3、Bルータ4、内部ネットワークである第1のネットワーク7に属するAサーバ30a、端末5a…5n、第1のネットワーク7に属するBサーバ30b及び端末6a…6nとを備えている。

【0033】

インターネット1は、第1のネットワーク7と第2のネットワーク9を繋げるための通信回線である。これはケーブル等で接続される専用回線、衛星通信等の遠距離無線通信、Bluetooth等の近距離無線通信等であっても構わない。

【0034】

Aルータ3及びBルータ4は、パケットをネットワーク層でルーティングする装置であり、第1のネットワーク7上のあらゆるノード間同士でのデータ転送を担当する。Aサーバ30aは、Aルータ3が管理するノードの中心となり処理を行うコンピュータである。Bサーバ30bは、Bルータ4が管理するノードの中心となり処理を行うコンピュータである。

【0035】

Aルータ3の下位ノードとしては、図2のように、Aサーバ30a、端末5a、5b、5cが存在する。Bルータ4の下位ノードには、図2のように、Bサーバ30b、端末6a、6b、6cが存在する。第1のネットワーク7の全ての装置はLANケーブル8にて接続されている。

【0036】

尚、通信装置 10a、10b、10c、…、境界ルータ 20、Aサーバ 30a 及び Bサーバ 30b 等の装置は、一般的なコンピュータに所定の機能を実現するソフトウェアプログラムをインストールすることにより実現される。

【0037】

また全ての装置のそれぞれのインターフェースは、図 2 に示すようにインターフェースアドレス（ここでは IPv6 アドレス）が付与されている。ここでは LAN ケーブル 8 の物理層はイーサネット（TM）であり、IPv6 アドレスが付与されていると仮定する。それぞれの IPv6 アドレスは、自インターフェースにあらかじめ付与された MAC アドレスを用いて 64 ビットのインターフェース識別子を生成する。インターフェース識別子を下位 64 ビットとして、またルータから受信したプレフィックスを上位 64 ビットとし、合計 128 ビットのアドレスを自動生成するものとする。

【0038】

IPv6 アドレスの形態にはリンクローカルアドレスやグローバルアドレスといった分類があるが、ここで説明するのは全てグローバルアドレスであると仮定する。

【0039】

境界ルータ 20 の下に属するネットワークを管理する管理者は、Aサーバ 30a のインターフェース及び、Bサーバのインターフェースに同一のエニキャストアドレス S を付与する。エニキャスト宛てのパケットは、経路的にもっとも近いエニキャストアドレスを持つインターフェースに配送される。

【0040】

ここでは境界ルータ 20 から見た場合に、経路的にもっとも近いエニキャストアドレス S をもつサーバは Aサーバ 30a であると仮定する。

【0041】

ここで A ルータ 3 及び B ルータ 4 は、それぞれ自ルータの下に属するノードがエニキャストアドレスを割り当てられているか否かを知っているものとする。例えば、A ルータ 3 は、Aサーバ 30a がエニキャストアドレス S を持っていることを示すテーブルを記憶しておく。同様に B ルータ 4 は Bサーバ 30b がエニキャストア

ドレスSを持っていることを示すテーブルを記憶しているとする。

【0042】

これらのテーブルはその前述の管理者が手動設定してもよいし、ルータとサーバ間で何らかのプロトコルを用いて自動設定としてもよい。

【0043】

(通信装置)

図1に示した通信装置10a、10b、10c、…は、それぞれ図3に示すように、入力装置11、出力装置12、通信制御装置13、主記憶装置14、処理制御装置(CPU)16等から構成される。CPU16は、送信手段16a、受信手段16b、第1の検出手段16c、第2の検出手段16d及び検証手段16e等を備えている。

【0044】

送信手段16aは、パケットのヘッダにある宛先アドレスをチェックし、その宛先アドレス宛にパケットを送信するモジュールである。受信手段16bは、パケットの応答として、送信相手のサーバ等より送信されてきた応答パケットを受信するモジュールである。

【0045】

第1の検出手段16cは、受信した応答パケットに含まれる、送信元アドレスを検出するモジュールである。第2の検出手段16dは、検出した送信元アドレスが、宛先アドレスと異なる場合、送信元アドレスに含まれるユニキャストアドレスを示す識別子を検出するモジュールである。検証手段16eは、識別子に基づいて応答パケットの検証を行うモジュールである。

【0046】

入力装置11は、キーボード、マウス等により構成される。又、通信制御装置13を介し外部装置より入力を行っても良い。ここで外部装置とは、CD-ROM、MO、ZIPなどの記憶媒体及びそのドライブ装置等を指す。出力装置12は、液晶ディスプレイ、CRTディスプレイ等の表示装置、インクジェットプリンタ、レーザープリンタ等の印刷装置等により構成される。

【0047】

通信制御装置 13 は、通信回線を介してデータを他の汎用機、サーバ等に送受信する為の制御信号を生成するモジュールである。主記憶装置 14 は、処理の手順を記述したプログラムや処理されるべきデータを一時的に記憶し、CPU 16 の要請に従ってプログラムの機械命令やデータを引き渡す。CPU 16 で処理されたデータは主記憶装置に書き込まれる。主記憶装置 14 と CPU 16 はアドレスバス、データバス、制御信号等で結ばれている。

【0048】

(通信装置による通信方法)

次に、通信装置 10a、10b、10c、…を用いた通信方法について、図 1 及び図 3 を参照しながら、図 6 のフローチャートを用いて説明する。

【0049】

(a) ステップ S101 では、図 3 に示す送信手段 16a が、パケットのヘッダにある宛先アドレスをチェックし、その宛先アドレス宛にパケットを送信する。パケットは図 1 に示すインターネット 1 等を介して宛先アドレス宛てに送信される。

【0050】

パケットを受け取ったサーバ等の相手装置は、このパケットに対する応答パケットを、通信装置 10a、10b、10c、…に向けて再び送信する。又、この送信の際に、サーバ等の相手装置は、応答パケットに自らの属するユニキャストアドレスを証明する識別子を付与する。

【0051】

(b) ステップ S102 では、受信手段 16b が、パケットの応答として、サーバ等の相手装置より送信されてきた応答パケットを受信する。

【0052】

(c) ステップ S103 では、第 1 の検出手段 16c が、受信手段 16b が受信した応答パケットに含まれる、送信元アドレスを検出する。これにより送信元の通信相手を特定することができる。

【0053】

(d) ステップ S104 では、検出した送信元アドレスが宛先アドレスと異なる

場合、第2の検出手段16dが、送信元アドレスに含まれるユニキャストアドレスを示す識別子を検出する。

【0054】

(e) ステップS105では、検証手段16eが、検出した識別子に基づいて、送信元のサーバ等の相手装置がなりすましでないことを認証する。

【0055】

このように通信装置10a、10b、10c、…にてユニキャストアドレス通信を示す識別子を検出することにより、ユニキャストアドレスと同等の安全性をユニキャストアドレスにて確保することが可能となる。

【0056】

(境界ルータ装置)

境界ルータ20は、図1に示すように、複数のユニキャストアドレス保有サーバ装置が属する第1のネットワーク7と、外部のネットワークである第2のネットワーク9との境界に位置する。境界ルータ20は、図4に示すように入力装置21、出力装置22、通信制御装置23、主記憶装置24、処理制御装置(CPU)26及び補助記憶装置27等から構成される。

【0057】

補助記憶装置27は、第1のネットワーク7内のインターフェースのアドレスを記憶する。CPU26は、第1の受信手段26a、第1の転送手段26b、第2の受信手段26c、検出手段26d、検証手段26e、転送制御手段26f及び第2の転送手段26gを備えている。第1の受信手段26aは、第2のネットワーク9側の通信装置10a、10b、10c、…から、複数のユニキャストアドレス保有サーバ装置宛の packets を受信するモジュールである。

【0058】

第1の転送手段26bは、パケットを複数のユニキャストアドレス保有サーバ装置の内、最も経路的に近距離にあるサーバ装置に転送するモジュールである。第2の受信手段26cは、経路的に最も近距離にあるサーバ装置から、パケットに対する応答パケットを受信するモジュールである。

【0059】

検出手段 26 d は、応答パケットに含まれる、ユニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出するモジュールである。検証手段 26 e は、検出手段 26 d において識別子が検出された場合、応答パケットがユニキャストアドレス保有サーバの内の 1 つのサーバから送信された応答パケットであることを検証するモジュールである。

【0060】

転送制御手段 26 f は、応答パケットを通信装置 10 a、10 b、10 c、…に転送するか否かを制御するモジュールである。第 2 の転送手段 26 g は、転送制御手段の制御によって、応答パケットを通信装置 10 a、10 b、10 c、…に転送するモジュールである。

【0061】

入力装置 21、出力装置 22、通信制御装置 23 及び主記憶装置 24 については、通信装置 10 a、10 b、10 c、…と同様であるため説明を省略する。

【0062】

(ルーティング方法)

次に境界ルータ 20 を用いたルーティング方法について図 7 のフローチャートを基に説明する。

【0063】

(a) ステップ S201 では、第 1 の受信手段 26 a が、図 1 のクライアント側の通信装置 10 a、10 b、10 c、…から、ユニキャストアドレス保有サーバ装置宛のパケットを受信する。

【0064】

(b) ステップ S202 では、第 1 の転送手段 26 b が、受信したパケットを、ユニキャストアドレス保有サーバ装置の内、最も経路的に近距離にあるサーバ装置に転送する。図 1 の場合、Aサーバ 30 a に転送する。

【0065】

(c) ステップ S203 では、第 2 の受信手段 26 c が、パケットに対する回答である、Aサーバ 30 a からの応答パケットを受信する。

【0066】

(d) ステップ S204 では、検出手段 26 d が、応答パケットに含まれる、ユニキャストアドレスとは異なる送信元アドレスが付与されていることを示す識別子を検出する。

【0067】

(e) ステップ S205 では、検証手段 26 e が、検出手段 26 d において識別子が検出された場合、応答パケットがユニキャストアドレス保有サーバの内の 1 つのサーバから送信された応答パケットであることを検証する。

【0068】

(f) ステップ S207 では、転送制御手段 26 f は、応答パケットを通信装置 10 a、10 b、10 c、…に転送するか否かを制御する。

【0069】

転送すると判断されると、ステップ S208 にて、第 2 の転送手段 26 g は、転送制御手段の制御によって、応答パケットを通信装置 10 a、10 b、10 c、…に転送する。又、転送しないと判断された場合、パケットは廃棄される。

【0070】

上記によると、境界ルータ 20 にてユニキャストアドレス通信を示す識別子のフィルタリングを実施することにより、ユニキャストアドレスと同等の安全性をユニキャストアドレスにて確保することが可能となる。

【0071】

(ユニキャストアドレスを保有するサーバ装置)

ユニキャストアドレスを保有するサーバ装置である A サーバ 30 a 及び B サーバ 30 b は、図 5 に示すように、入力装置 31、出力装置 32、通信制御装置 33、主記憶装置 34、処理制御装置 (CPU) 36 及び識別子記憶装置 37 等から構成される。

【0072】

識別子記憶装置 37 は、ユニキャストアドレスを保有することを示す識別子を記憶する。

【0073】

CPU 36 は、受信手段 36 a、識別子付与手段 36 b 及び送信手段 36 c を

備える。受信手段36 aは、第2のネットワーク9に接続された通信装置10 a、10 b、10 c、…からエニキャストアドレス宛に送信されたパケットを受信するモジュールである。

【0074】

識別子付与手段36 bは、パケットに応答する応答パケットの送信元アドレスに、エニキャストアドレスを保有することを示す識別子を付与するモジュールである。送信手段36 cは、応答パケットを通信装置10 a、10 b、10 c、…へ送信するモジュールである。

【0075】

入力装置31、出力装置32、通信制御装置33及び主記憶装置34に関しては通信装置10 a、10 b、10 c、…と同様であるため説明を省略する。

【0076】

(エニキャストアドレスを保有するサーバ装置の通信方法)

次に、Aサーバ30 a及びBサーバ30 bの通信方法について説明する。

【0077】

(a) ステップS301では、受信手段36 aが、通信装置10 a、10 b、10 c、…から、インターネット1を介して、エニキャストアドレス宛に送信されたパケットを受信する。

【0078】

(b) ステップS302では、識別子付与手段36 bが、パケットに応答する応答パケットの送信元アドレスに、エニキャストアドレスを保有することを示す識別子を付与する。この識別子は識別子記憶装置37に記憶される識別子を使用する。

【0079】

(c) ステップS303では、送信手段36 cが、識別子を付与した応答パケットを、通信装置10 a、10 b、10 c、…へ送信する。

【0080】

上記によると、Aサーバ30 aがエニキャスト通信を示す識別子を付与することにより、他の装置がフィルタリングを行うことが可能となり、ひいてはユニキ

キャストアドレスと同等の安全性をエニキャストアドレスにて確保することが可能となる。

【0081】

(通信装置、境界ルータ装置及びサーバ装置を使用する通信方法)

以下、図1に示す通信装置10a、10b、10c、…を用いてAサーバ30a宛てにパケットの送受信を行う過程について図9を用いて説明する。

【0082】

(a) ステップS401にて、通信装置10a、10b、10c、…の入力装置11等を介してパケット送信要求が入力されると、送信手段16aが、パケットのヘッダにあるAサーバ30aの宛先アドレスをチェックし、その宛先アドレス宛にパケットを送信する。パケットはインターネット1を通じて宛先アドレス宛てに送信される。Aサーバが属する第1のネットワーク7にて受信されたパケットはステップS402のように境界ルータ20及びAルータ3に転送され、最終的に宛先アドレスのAサーバ30aに送信される。

【0083】

(b) ステップS403にて、Aサーバ30aの受信手段36aがパケットを受信する。この後ステップS404にて、識別子付与手段36bは返信するパケットに識別子を付与する。この識別子は識別子記憶装置37に記憶しているものを使用する。

【0084】

識別子付与後、ステップS405にて、送信手段36cは、通信装置10a、10b、10c、…に向けて応答パケットを送信する。応答パケットは、Aルータ3にルーティングされ、境界ルータ20に送信される。

【0085】

(c) ステップS406にて、境界ルータ20の第2の受信手段26cが応答パケットを受信すると、ステップS407にて、検出手段26dが応答パケットよりエニキャストアドレスを示す識別子を検出する。

【0086】

(d) ステップS408では、検証手段26eが、検出された識別子が適切であ

るか否かの検証を行う。検証の結果、パケットが適切である場合、ステップ S 4 1 0 にて、第 2 の転送手段 2 6 g が、通信装置 1 0 a、1 0 b、1 0 c、…に向けて、インターネット 1 を介し、応答パケットを送信する。パケットが適切でない場合、そのパケットはステップ S 4 1 1 にて廃棄される。

【0087】

(e) ステップ S 4 1 2 では、通信装置 1 0 a、1 0 b、1 0 c、…の受信手段 1 6 b が、応答パケットを受信する。第 1 の検出手段 1 6 c が、受信された応答パケットの送信元アドレスを検出し、第 2 の検出手段 1 6 d が、応答パケットよりユニキャストアドレスを示す識別子を検出する。

【0088】

(f) ステップ S 4 1 3 にて、ユニキャストアドレスを示す識別子を保有しているか否かを基に、この応答パケットが、適切なサーバ、つまり A サーバ 3 0 a から送信されたものかどうかの検証を行う。適切な識別子を保有している場合、ステップ S 4 1 4 にてこの応答パケットの読込を行い、適切な識別子を保有していない場合、ステップ S 4 1 5 にてこの応答パケットを廃棄する。

【0089】

上記によると、A サーバ 3 0 a がユニキャスト通信を示す識別子を付与し、通信装置 1 0 a、1 0 b、1 0 c、…及び境界ルータ 2 0 においてこの識別子のフィルタリングを実施することにより、ユニキャストアドレスと同等の安全性をユニキャストアドレスにて確保することが可能となる。

【0090】

【発明の効果】

本発明により、ユニキャストアドレス利用時のなりすまし攻撃に対し、ユニキャストアドレスと同等の耐性が得られ、ユニキャストアドレスと同等の安全性の上で、ユニキャストアドレス通信の利点である、プラグアンドプレイ機能を用いた不特定多数の通信装置、通信端末との通信を行うことが可能な通信装置、境界ルータ装置、サーバ装置、通信システム、通信方法、ルーティング方法、通信プログラム及びルーティングプログラムを提供することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施の形態に係る通信システムの概要図である。

【図 2】

本発明の一実施の形態に係るエニキャストアドレス通信の構成図である。

【図 3】

本発明の一実施の形態に係る通信装置の構成図である。

【図 4】

本発明の一実施の形態に係るルータ装置の構成図である。

【図 5】

本発明の一実施の形態に係るサーバ装置の構成図である。

【図 6】

本発明の一実施の形態に係る通信装置の通信方法を示すフローチャートである。

【図 7】

本発明の一実施の形態に係るルータ装置のルーティング方法を示すフローチャートである。

【図 8】

本発明の一実施の形態に係るサーバ装置の通信方法を示すフローチャートである。

【図 9】

本発明の一実施の形態に係る通信システムの通信方法を示すフローチャートである。

【符号の説明】

- 1…インターネット
- 3…A ルータ
- 4…B ルータ
- 5 a、5 b、5 c…端末
- 6 a、6 b、6 c…端末
- 7…第 1 のネットワーク

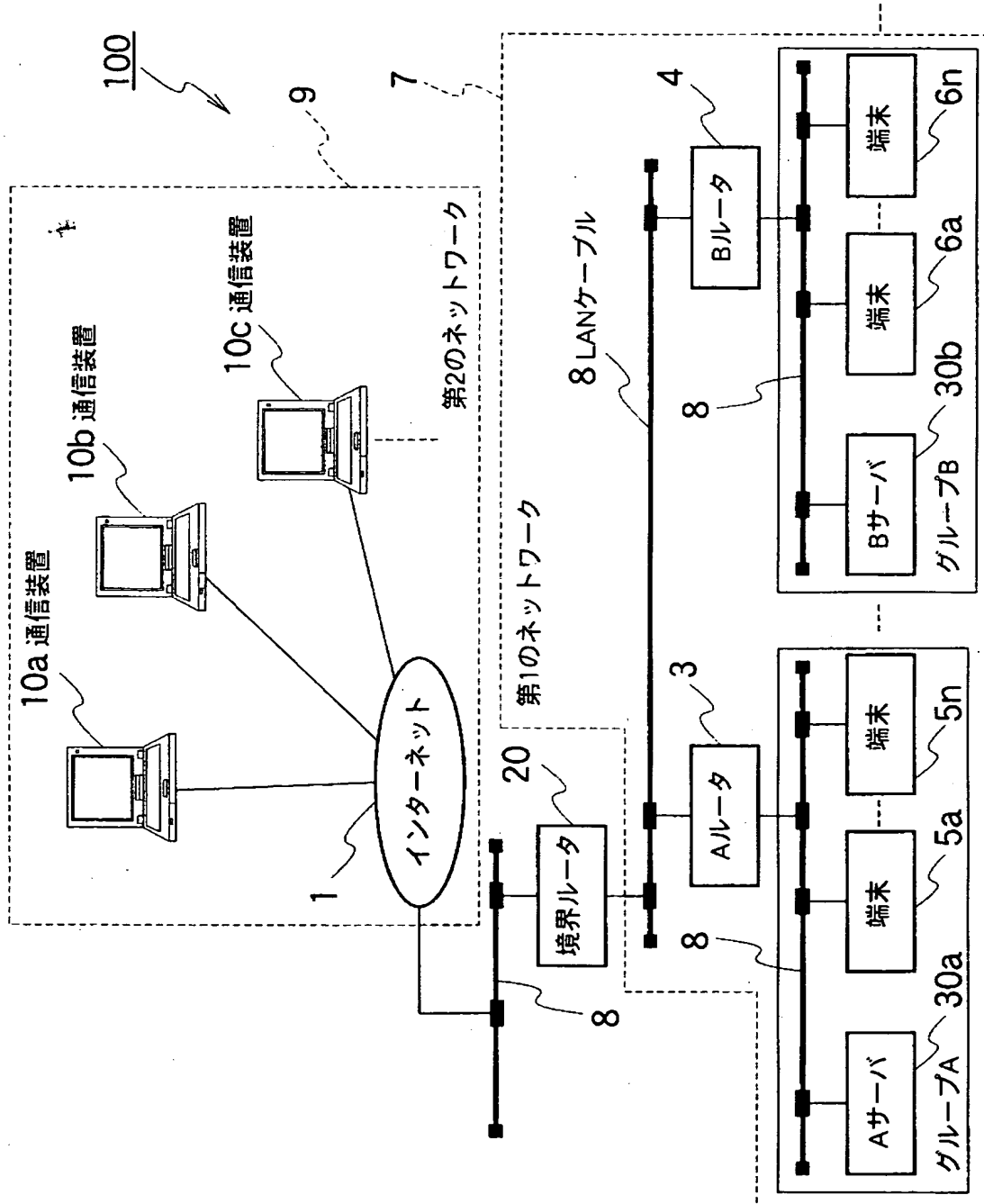
8…LANケーブル

9…第2のネットワーク

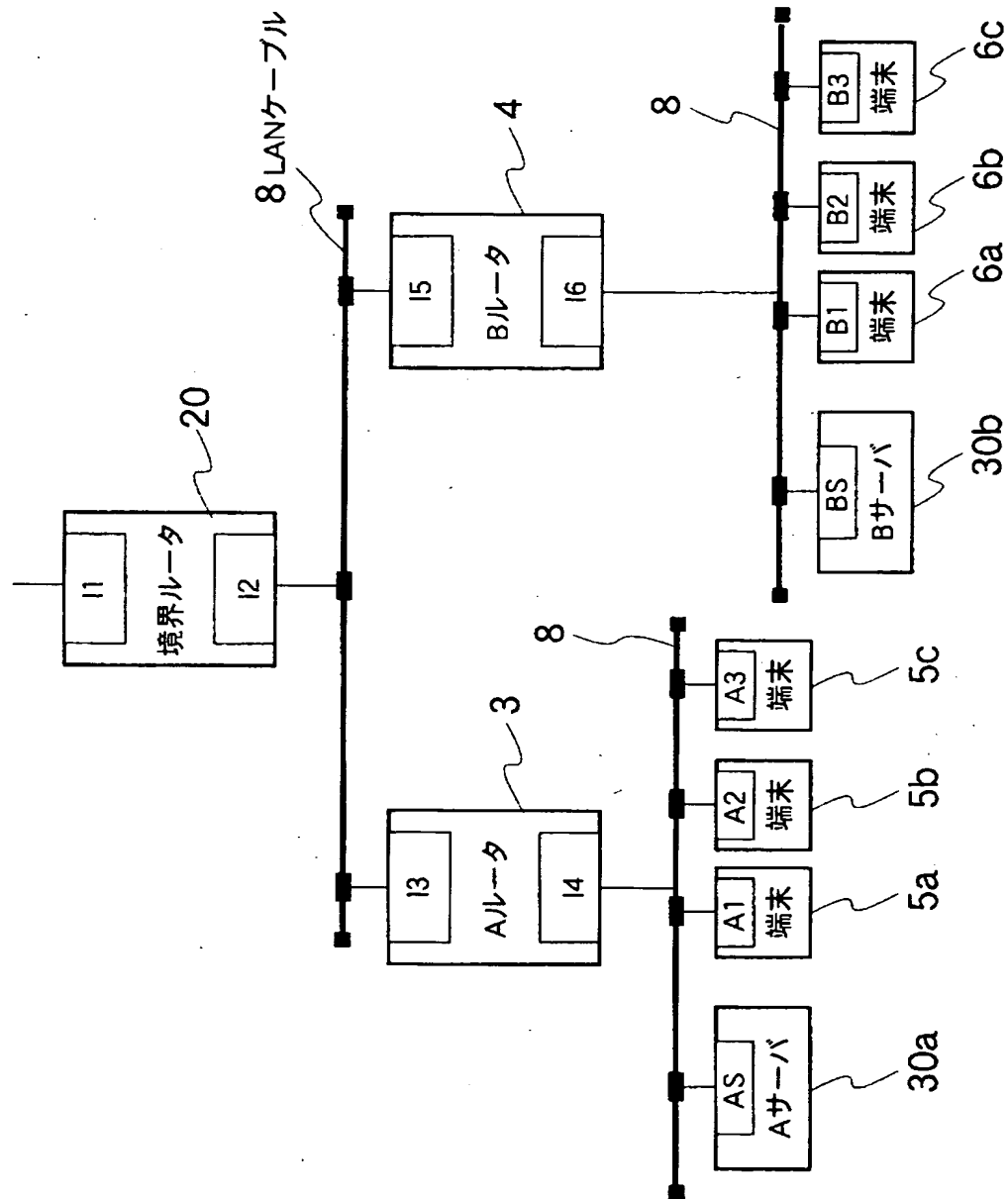
10 a、10 b、10 c……通信装置

【書類名】 図面

【図1】

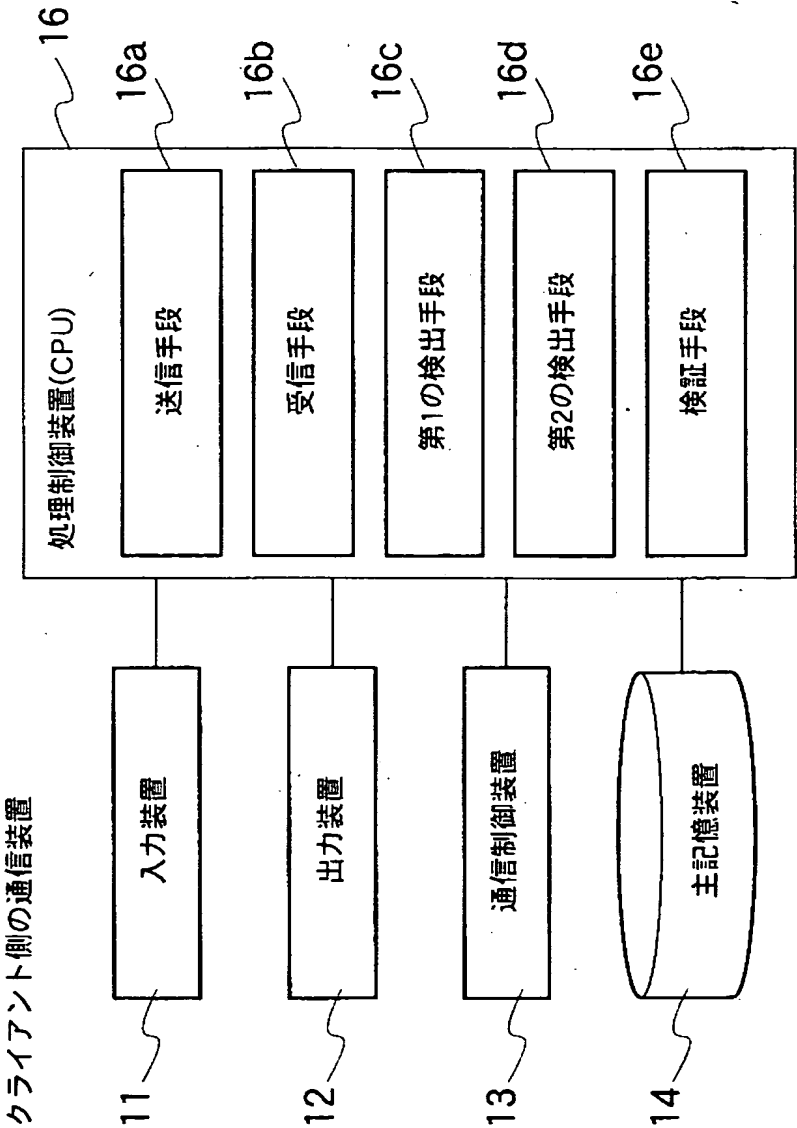


【図 2】

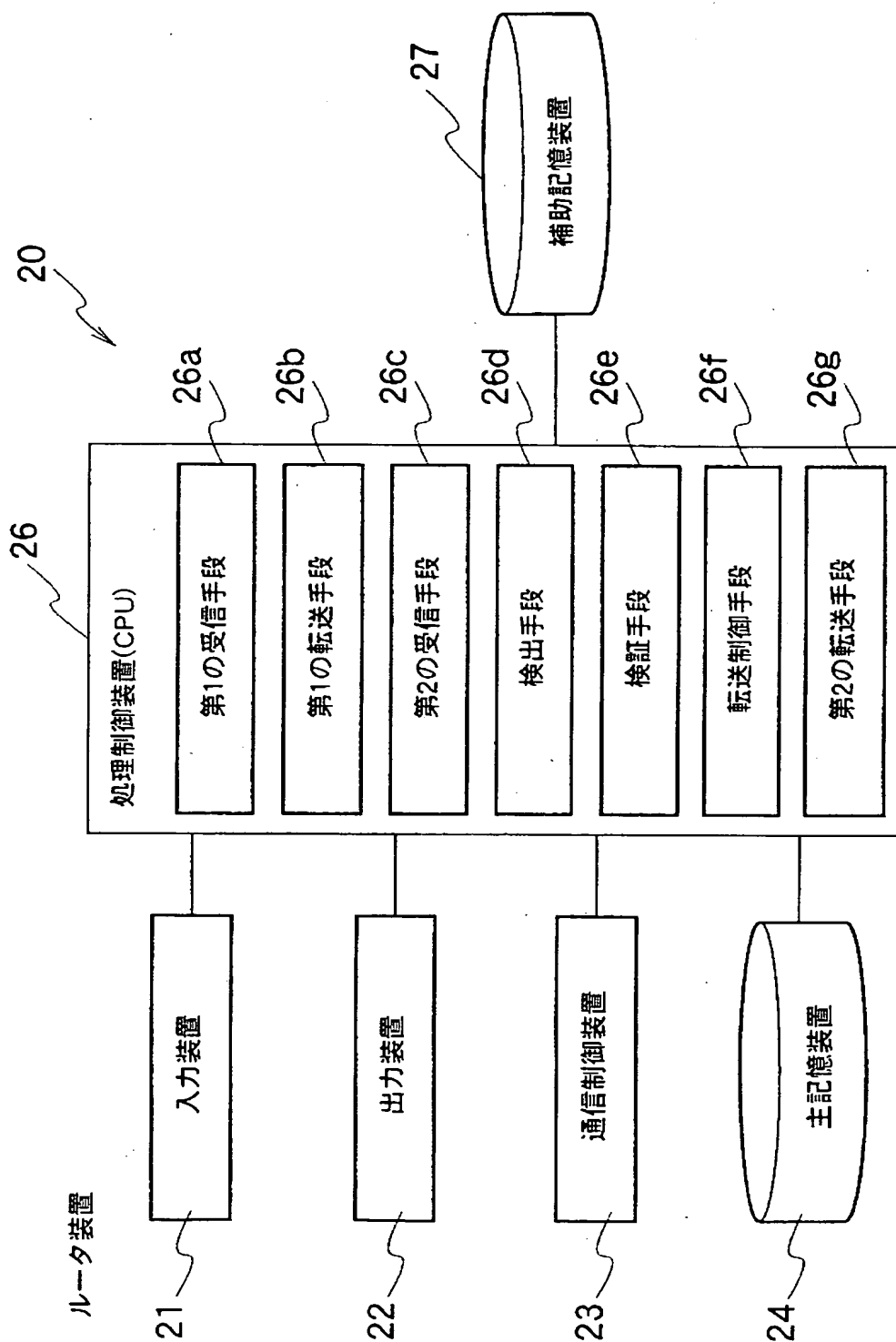


【図 3】

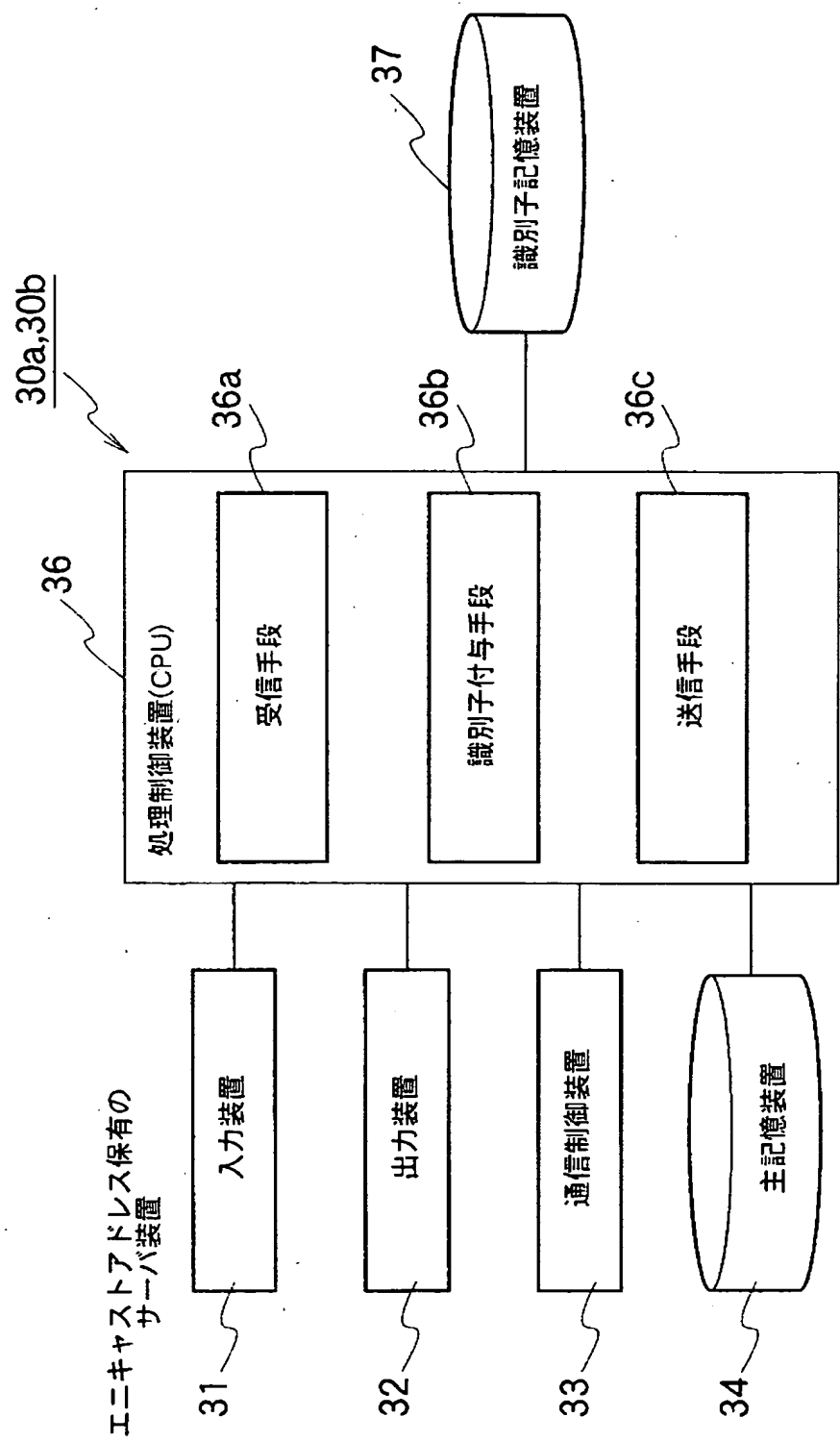
10a, 10b, 10c, ...



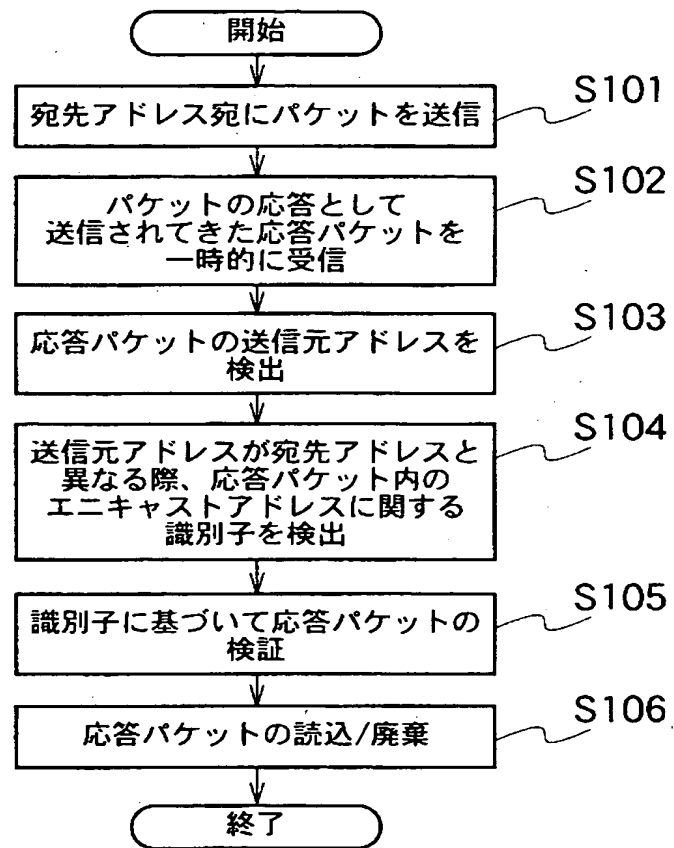
【図 4】



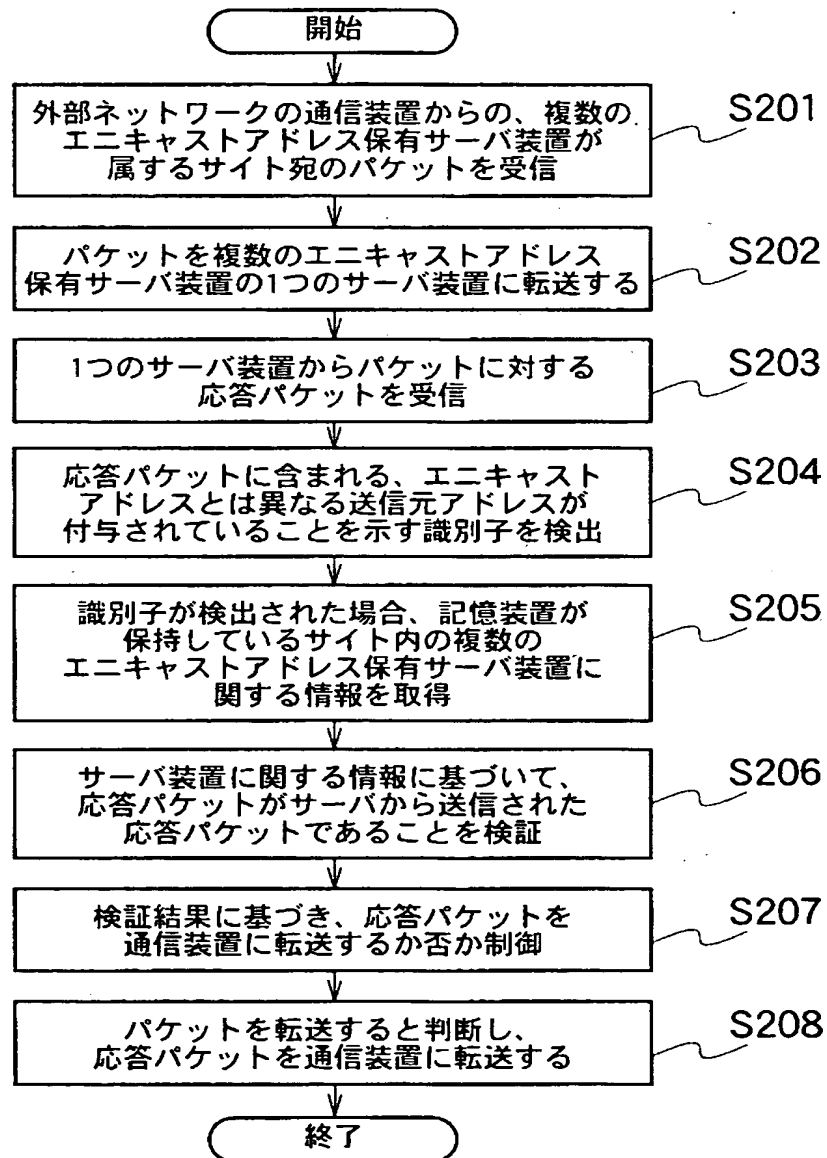
【図 5】



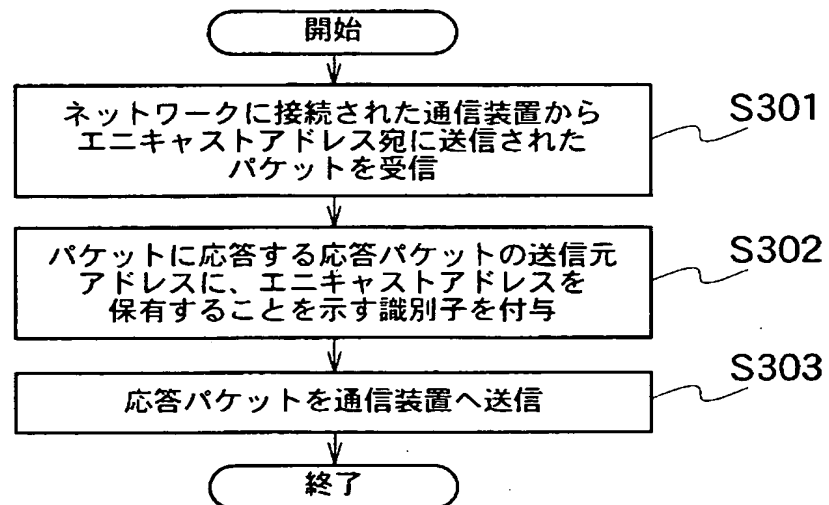
【図 6】



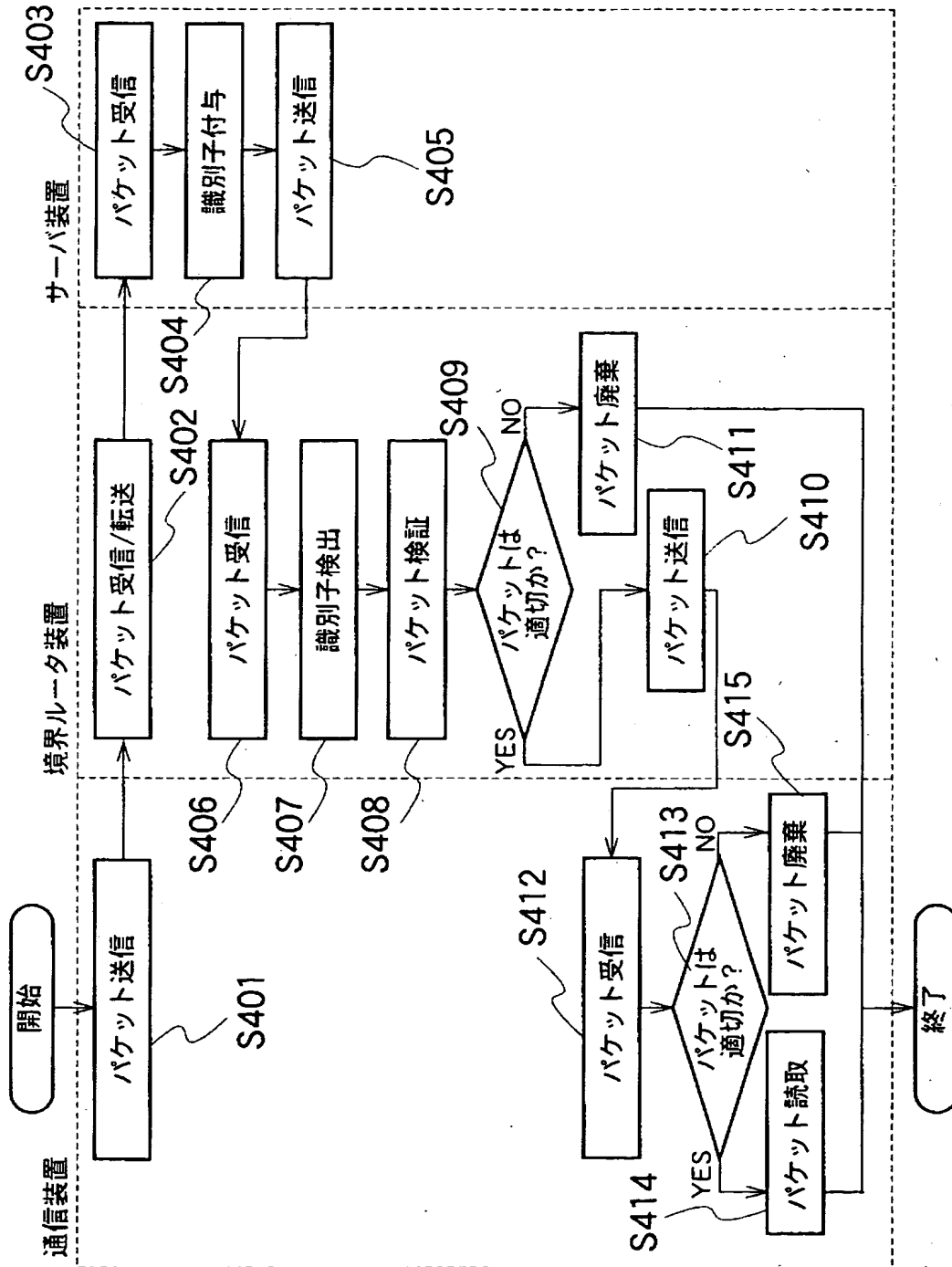
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 エニキャストアドレスを用いたサービスにおいて、送信元の正当性を検証し、なりすましによる被害を防止する通信装置、境界ルータ装置、サーバ装置、通信システム、通信方法、ルーティング方法、通信プログラム及びルーティングプログラムを提供する。

【解決手段】 応答パケットの送信元アドレスを検出し、送信元アドレスが、宛先アドレスと異なる場合に応答パケットのエニキャストアドレスを示す識別子を検出し、応答パケットの検証を行う通信装置 10 a、10 b、10 c、…と応答パケット内の識別子を検出し、予め記憶されたサーバ装置に関する情報より、応答パケットがサーバから送信された応答パケットであることを検証する境界ルータ 20 と、応答パケットの送信元アドレスに、エニキャストアドレスを示す識別子を付与する手段を持つ A サーバ 30 a 等を用いて送受信の際にフィルタリングを行う。

【選択図】 図 1

特願 2002-329950

出願人履歴情報

識別番号

[000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝
2. 変更年月日 2003年 5月 9日
[変更理由] 名称変更
住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝